**Czy nowe funkcje bezpieczeństwa Androida 4.4 mają znaczenie?**

**Niedawno firma Google opublikowała wersję 4.4 (KitKat) swojego mobilnego systemu operacyjnego Android. Wśród usprawnień pojawiły się zmiany związane z bezpieczeństwem. Stefan Tanase, ekspert z Kaspersky Lab, analizuje, jaki wpływ na ogólną ochronę urządzeń mobilnych z Androidem ma najnowsza aktualizacja.**

Główne udoskonalenia w zakresie bezpieczeństwa Androida 4.4 (KitKat) można podzielić na dwie kategorie:

**1. Certyfikaty cyfrowe**

Android 4.4 ostrzeże użytkownika, jeżeli do urządzenia zostanie dodane nowe centrum certyfikacji, ułatwiając tym samym zidentyfikowanie ataków wewnątrz sieci lokalnych. Jednocześnie nowa funkcja bezpieczeństwa (Google Certificate Pinning) utrudni zaawansowanym cyberprzestępcom przechwytywanie ruchu sieciowego do i z usług Google’a. Jedynie certyfikaty umieszczone na białej liście będą mogły łączyć się z określonymi domenami Google’a.

**2. Wzmocnienie systemu operacyjnego**

Dzięki wprowadzonym udoskonaleniom nowy Android może skuteczniej blokować szkodliwe programy, które usiłują uzyskiwać dostęp do systemu na poziomie administracyjnym (root). Dodatkowo, w wersji 4.4 Androida znacznie trudniej jest przeprowadzić atak polegający na przepełnieniu bufora.

Warto zwrócić uwagę, że eskalacja przywilejów i przepełnienie bufora to techniki wykorzystywane do popularnego rootowania urządzeń z Androidem, na które wielu użytkowników decyduje się, by mieć możliwość szerszej personalizacji smartfonów i tabletów. Po aktualizacji do wersji 4.4 proces ten będzie znacznie trudniejszy.

Czy teraz będzie bezpieczniej?

Z punktu widzenia szkodliwego oprogramowania wspomniane usprawnienia tak naprawdę nie robią wielkiej różnicy. Najpopularniejsze źródło infekcji Androida pozostaje takie samo: są to nieoficjalne aplikacje pobierane przez użytkowników ze sklepów osób trzecich oraz zainfekowane programy, na które można trafić w oficjalnym sklepie Google Play. Pod tym względem nic się nie zmieni.

Jednym z największych problemów w ekosystemie Androida jest duża liczba różnych wersji tego systemu operacyjnego, łącznie z bardzo starymi, które nadal można znaleźć na urządzeniach mobilnych użytkowników – zjawisko to zwane jest fragmentacją wersji. Szacuje się, że ponad 25% użytkowników nadal wykorzystuje Androida 2.3, który został opublikowany wiele lat temu. Jest to poważny problem z punktu widzenia bezpieczeństwa.

Być może najważniejszą zmianą, jaką oferuje KitKat, jest zmniejszone zużycie zasobów. Android 4.4 może działać na urządzeniach posiadających zaledwie 512 MB pamięci RAM, co w przypadku sprzętu z wysokiej półki oznacza szybsze działanie i dłuższą pracę na baterii, natomiast w przypadku urządzeń z mniejszą ilością zasobów – możliwość wykorzystywania nowoczesnego, bezpieczniejszego systemu operacyjnego.

*„Prawdziwym problemem jest fakt, że większość nietechnicznych użytkowników będzie musiała polegać na producentach sprzętu w celu uzyskania aktualizacji Androida”* - komentuje Stefan Tanase, ekspert z Kaspersky Lab. *„Ja na przykład mam stosunkowo starego smartfona czołowego producenta telefonów komórkowych z Korei Południowej, który nie otrzymuje aktualizacji od wersji 2.3.3. Smutna prawda jest taka, że wielu producentów telefonów komórkowych celowo wstrzymuje aktualizacje, aby nakłonić klientów do zakupienia nowszych urządzeń, a to w znaczny sposób zwiększa ryzyko, na jakie narażeni są wszyscy użytkownicy”.*

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>.